Measuring Evidential Weight in Digital Forensic Investigations:

a Role for Bayesian Networks in Digital Forensic Triage

Richard E Overill

Department of Informatics, King's College London, Strand, London WC2R 2LS, UK

richard.overill@kcl.ac.uk

Kam-Pui Chow

Department of Computer Science, University of Hong Kong, Pokfulam Road, Hong Kong

chow@cs.hku.hk

Abstract **–** a method for obtaining a quantitative measure of the relative weight of each individual item of evidence in a digital forensic investigation by means of a Bayesian network is described. The resulting evidential weights can then be used to determine a near-optimal cost-effective triage scheme for the investigation in question.

Keywords: digital forensics**;** quantitative metric; Bayesian network; evidential weight; cost-effective triage scheme.

Introduction and Background

Until recently, an inability to reliably quantify the relative plausibility of alternative hypotheses purporting to explain the existence of the *totality* of the recovered digital evidence in a criminal investigation has hindered the development of digital forensics into a mature scientific and engineering discipline from the qualitative craft that originated in the mid-1980s [1]. Such a rigorous science and engineering oriented approach should not only provide numerical results but should also quantify the confidence limits, sensitivities and uncertainties associated with these results. However, beyond the works cited in the present contribution, there appears to be a dearth of research literature devoted to developing such a rigorous approach to digital forensic investigations.

Posterior probabilities, likelihood ratios (LRs) and odds, generated using technical approaches such as Bayesian Networks (BNs), are capable of providing digital forensic investigators, law enforcement officers and legal personnel with a quantitative scale or metric against which to assess the plausibility of an investigatory hypothesis which may be linked to the likelihood of a successful prosecution, or indeed the merit of a not-guilty plea. This approach is sometimes referred to as *digital meta-forensics*; some examples can be found in [2, 3].

A second and closely related issue involves reliably quantifying the relative weight of each of the *individual* items of digital evidence recovered during a criminal investigation. This is particularly important from the perspective of digital forensic triage, *i.e.* the prioritisation

strategy for searching for digital evidence, in the context of the ever-increasing volumes of data and varieties of device that are routinely seized for examination [4]. The economics of digital forensics, also known as *digital forensonomics* [5], provides for the possibility of a quantitative basis upon which to prioritise the search for digital evidence during a criminal investigation, by making use of such well-known concepts from the field of Economics as Return-on-Investment (RoI) or, essentially equivalently, Cost-Benefit Ratio (CBR).

In this approach, a list of all the expected items of digital evidence for the hypothesis being investigated is drawn up. For each item of digital evidence, two attributes are required: (i) its *cost*, which is in principle relatively straightforward to quantify as it is usually measured in terms of the resources required to locate, recover and analyse that item of digital evidence, typically investigator hours plus any specialist equipment hire-time needed; (ii) its *relative weight*, which measures the contribution that the presence of that item of digital evidence makes towards supporting the hypothesis, and until now it is usually based on the informal opinions or consensus of experienced digital forensic investigators [6].

The principal contributions of this short paper are: (i) to demonstrate that a *quantitative* measure of the relative weight of each item of digital evidence in a particular investigation can be obtained in a straightforward manner from the Bayesian network (BN) representing the hypothesis underpinning that investigation; and (ii) to demonstrate that these evidential weights can be employed to create a near-optimal cost-effective evidence search list for the triage phase of the digital forensic investigation process.

Methodology

Bayesian networks (BNs) were first proposed by Judea Pearl [7], based upon the concept of conditional probability originated by Thomas Bayes in the eighteenth century [8]. Formally speaking, a BN is a directed acyclic graph (DAG) representation of the conditional dependency relationships between entities such as events, observations or outcomes. Visually, a BN typically resembles an inverted tree. In the context of digital forensic investigations, the root node of the BN represents the overall hypothesis underpinning the investigation in question, the child nodes of the root node represent the sub-hypotheses which contribute to the overall hypothesis, and the leaf nodes represent the items of digital evidence that are associated with each of the sub-hypotheses. After populating the interior nodes with conditional probabilities (likelihoods) and assigning prior probabilities to the root node, the BN can then propagate these probabilities using the rules of Bayesian inference to produce a posterior probability for the root hypothesis. However, it is the architecture of the BN together with the definition of each sub-hypothesis and its associated evidential traces, which together define the hypothesis characterising the specific investigation. The first application of a BN to a specific digital forensic investigation appears to be that reported in [2]. Figure 1 illustrates an example of a BN applied to a particular digital forensic investigation.

The posterior probability output by the BN when all of the expected items of digital evidence are present is compared with the posterior probability of the BN when item *i* of the digital evidence is absent (but all the other expected evidential items are present); the difference between, and the ratio of, these two quantities both provide a direct measure of the relative weight of item *i* of the digital evidence in the particular context of the hypothesis of the investigation represented by the BN. Thus the relative weight of evidential item *i* can be written as:

$$(\text{relative-weight})_i \propto \text{posterior-probability} - (\text{posterior-probability})_i \quad (1)$$

or, in normalized form, as:

$$(\text{relative-weight})_i \propto \text{I} - \{(\text{posterior-probability})_i \,/\, \text{posterior-probability}\} \quad (2)$$

or alternatively as:

$$(\text{relative-weight})_i \propto \text{posterior-probability} \,/\, (\text{posterior-probability})_i \quad (3)$$

where $(\text{posterior-probability})_i$ signifies the posterior probability output by the BN when item *i* of the digital evidence is absent. From a ranking perspective, any one of equations (1), (2) or (3) could be used since in each case the relative weight of evidential item *i* increases monotonically with the difference between the posterior probabilities. For the remainder of this work we will continue to employ equation (1).

For a BN involving n_e items of digital evidence it is necessary to perform $(n_e + 1)$ executions of the BN. Once all of the relative evidential weights have been obtained in this manner using any one of equation (1), (2) or (3), the RoI and CBR for item *i* of the expected digital evidence in the hypothesis are given by the following two equations, respectively [5]:

$$(\text{RoI})_i \propto (\text{relative-weight})_i \,/\, [(\text{examiner-hours})_i \times (\text{hourly-cost}) + (\text{equipment-cost})_i] \quad (4)$$

$$(\text{CBR})_I \propto [(\text{examiner-hours})_i \times (\text{hourly-cost}) + (\text{equipment-cost})_i] \,/\, (\text{relative-weight})_I \quad (5)$$

Results and Discussion

As an illustrative application of the proposed approach we have taken the real-world criminal case of the illegal uploading of copyright protected material via the peer-to-peer BitTorrent network [2, 10]. The freely available BN simulator MSBNx [11] from Microsoft Research was used to perform all the required calculations initially; these results were subsequently verified independently using the free version of AgenaRisk [12]. A previous sensitivity analysis performed on the BitTorrent BN [9] demonstrated that the posterior probabilities, and hence the relative evidential weights derived from them, are stable to within $<\pm 0.5\%$.

The ranked evidential weights of the 18 items of digital evidence shown in Figure 1 are listed in Table 1, together with their estimated relative costs [6] and their associated RoIs

and CBRs as given by equations (4) and (5) respectively. The relative evidential recovery costs for the BN are taken from [6] and were estimated by experienced digital forensic investigators from the Hong Kong Customs & Excise Department IPR Protection group, taking into account the typical forensic examiner time required together with any specialist equipment utilisation needed. In the present approach it has been assumed that the typical cost of locating, recovering and analysing each individual item of digital evidence is fixed, although it can be envisaged that under certain circumstances an evidentiary cost could be variable, for example, if its recovery required the invocation of a mutual legal assistance treaty (MLAT) with law enforcement officers in another jurisdiction.

The relative evidential weights in Table 1 can be used to create an *evidence search list*, with the evidential items ordered first by decreasing relative weight and, within that, either by decreasing RoI or, equivalently, by increasing CBR. This search list can be used to guide the course of the triage phase of the digital forensic investigation in a near-optimal cost-effective manner by ensuring that evidential 'quick wins' (or 'low-hanging fruit') are processed early on in the investigation whilst evidence of low relative weight which is costly to obtain is relegated until later on, when it may become clearer whether or not the support of this evidence will be crucial to the overall support for the investigative hypothesis.

The advantages of a procedure such as this are that if an item of evidence of high relative weight is not recovered, this fact will be detected early on during the investigation and could result in the investigation being de-prioritised or even abandoned at an early stage, before valuable resources (of time, effort, equipment, *etc.*) have been expended unnecessarily. In addition, it may be possible to terminate the investigation without the need to search for an item of evidence of low relative weight with a high recovery cost (*e.g.* the requirement to use a scanning electron microscope to detect whether or not a solid-state memory latch or gate is charged), as a direct consequence of the Law of Diminishing Returns.

In the BitTorrent example illustrated above, if evidential item E_{18} could not be recovered, the outcome for the investigation would probably be serious and might well lead to its immediate de-prioritisation or even abandonment, whereas the absence of evidential items E_5 or E_7 would make very little difference to the overall support for the digital forensic investigation hypothesis.

A further possible refinement of the scheme outlined above can be introduced by considering the role of any potentially exculpatory (*i.e.* exonerating) items of evidence in the investigatory context. Such evidence might be, for example, that CCTV footage reliably places the suspect far from the presumed scene of the digital crime at the material time. The existence of any such evidence would by definition place the investigatory hypothesis in jeopardy. Therefore if any such potential evidence could be identified in advance then a search for this potentially exculpatory evidence could be undertaken either before or in parallel with the search for evidential items in the triage schedule. However, since by definition the BN for the investigatory hypothesis would not contain any exculpatory evidential items, it cannot be used directly to obtain the relative weights of any such items

of exculpatory evidence. Hence it is not possible to formulate a cost-effective search strategy for these items on the basis of the BN itself.

Summary and Conclusions

A method to obtain numerically the relative weight for each item of digital evidence from the associated BN has been outlined and illustrated by applying it to the commonly occurring criminal case of piracy of copyright protected material using the BitTorrent P2P network. By considering the corresponding RoIs or CBRs, a near-optimal cost-effective digital forensic triage search strategy for this exemplar case can be constructed, which eliminates unnecessary utilisation of scarce resources (of time, effort, equipment, *etc.*) in today's overstretched, under-resourced, digital forensic investigation laboratories.

References

[1] F Cohen, Digital Forensic Evidence Examination, 4th edition, 2013, http://all.net/books/2013-DFE-Examination.pdf

[2] M Kwan, K-P Chow, F Law and P Lai. Reasoning about Evidence using Bayesian Networks, Advances in Digital Forensics IV, Proc. IFIP WG11.9 annual conference January 2008, Tokyo, pp.141-155.

[3] Y K Kwan, R E Overill, K-P Chow, J A M Silomon, H Tse, Y W Law and K Y Lai, Evaluation of Evidence in Internet Auction Fraud Investigations, Proc.6th Annual IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, 3-6 January 2010, Advances in Digital Forensics VI, Ch.7, pp.95-106, Springer (2010).

[4] Digital Investigation, Vol.10, Iss.2 (2013), special issue on triage.

[5] R E Overill, Digital Forensonomics - the Economics of Digital Forensics, Proc. 2nd International Workshop on Cyberpatterns (Cyberpatterns 2013), Abingdon, UK, 8-9 July 2013.

[6] R E Overill, Y K Kwan, K-P Chow, K Y Lai and Y W Law, A Cost-Effective Digital Forensics Investigation Model, Proc. 5th Annual IFIP WG 11.9 International Conference on Digital Forensics, Orlando, Florida, USA, 25-28 January 2009, Advances in Digital Forensics V, Ch.15, pp.193-202, Springer (2009).

[7] J Pearl, Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference, Morgan Kaufman, San Mateo, CA, 1988.

[8] T Bayes, An essay towards solving a Problem in the Doctrine of Chances, Phil. Trans. Roy. Soc. Lond., vol.53, p.370, 1763.

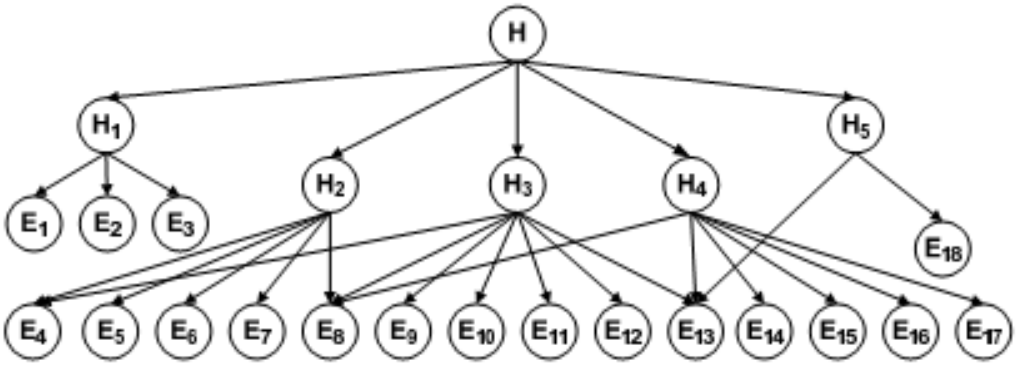
[9] R E Overill, J A M Silomon, Y K Kwan, K-P Chow, Y W Law and K Y Lai, Sensitivity Analysis of a Bayesian Network for Reasoning about Digital Forensic Evidence, Proc. 4th International Workshop on Forensics for Future Generation Communication Environments (F2GC-2010), in Proc. HumanCom-2010: 3rd International Conference on Human-Centric Computing, Cebu, Philippines, 11-13 August 2010, IEEE Press, pp.228-232.

[10] HKSAR *versus* Chan Nai Ming, Reasons for Verdict, TMCC 1268/2005, Hong Kong, 24 October 2005 and 7 November 2005.
http://www.hklii.hk/hk/jud/en/hksc/2005/TMCC001268_2005.html

[11] Microsoft Research, MSBNx: Bayesian Network Editor and Tool Kit, Microsoft Corporation, Redmond, Washington, USA, 2001.
http://www.research.microsoft.com/adapt/MSBNx

[12] AgenaRisk 7.0, Bayesian Network and Simulation Software for Risk Analysis and Decision Support, Agena Ltd., Cambridge, UK, 2016.
http://www.agenarisk.com/products/free_download.shtml

Figure 1: BN for the BitTorrent investigation [2]



HYPOTHESES:

H	The seized computer was used as the initial seeder to share the pirated file on a BitTorrent network
H_1	The pirated file was copied from the seized optical disk to the seized computer
H_2	A torrent file was created from the copied file
H_3	The torrent file was sent to newsgroups for publishing
H_4	The torrent file was activated, which caused the seized computer to connect to the tracker server
H_5	The connection between the seized computer and the tracker was maintained

EVIDENCE:

E_1	Modification time of the destination file equals that of the source file
E_2	Creation time of the destination file is after its own modification time
E_3	Hash value of the destination file matches that of the source file
E_4	BitTorrent client software is installed on the seized computer
E_5	File link for the shared file is created
E_6	Shared file exists on the hard disk
E_7	Torrent file creation record is found
E_8	Torrent file exists on the hard disk
E_9	Peer connection information is found
E_{10}	Tracker server login record is found
E_{11}	Torrent file activation time is corroborated by its MAC time and link file
E_{12}	Internet history record about publishing website is found
E_{13}	Internet connection is available
E_{14}	Cookie of the publishing website is found
E_{15}	URL of the publishing website is stored in the web browser
E_{16}	Web browser software is available
E_{17}	Internet cache record about the publishing of the torrent file is found
E_{18}	Internet history record about the tracker server connection is found

BN Post.Prob.	**Evidence**	**Rel.Evid.Weight**	**Rel.Est.Cost**	**RoI**	**CBR**
[9, Table A1]	**Item**	**Eq.(1)**	[6, Table 1]	×100	×0.01
0.9255	**–**	**–**	**–**	**–**	**–**
0.8623	E_{18}	0.0632	1.5	4.214	0.237
0.8990	E_{13}	0.0265	1.5	1.767	0.566
0.9109	E_{3}	0.0146	1.0	1.459	0.685
0.9158	E_{1}	0.0097	1.0	0.968	1.033
0.9158	E_{2}	0.0097	1.0	0.968	1.033
0.9239	E_{11}	0.0016	2.0	0.082	12.20
0.9240	E_{6}	0.0015	1.0	0.151	6.622
0.9242	E_{16}	0.0013	1.0	0.127	7.874
0.9247	E_{12}	0.0008	1.5	0.050	20.00
0.9248	E_{9}	0.0007	2.0	0.036	27.78
0.9248	E_{10}	0.0007	1.5	0.047	21.28
0.9249	E_{8}	0.0006	1.0	0.062	16.13
0.9251	E_{15}	0.0004	1.0	0.040	25.00
0.9251	E_{17}	0.0004	1.5	0.027	37.04
0.9252	E_{14}	0.0003	1.5	0.021	47.62
0.9252	E_{4}	0.0003	2.0	0.013	76.92
0.9253	E_{5}	0.0002	1.0	0.015	66.67
0.9254	E_{7}	0.0001	1.5	0.007	142.9

Table 1: Posterior probabilities, relative evidential weights, relative estimated costs, RoIs and CBRs for each expected item of digital evidence in the BitTorrent investigation.